(51) International Patent Classification 5 : H04Q 7/04, H04B 7/26	A1	(11) International Publication Number: WO 93/17529 (43) International Publication Date: 2 September 1993 (02.09.93)

(21) International Application Number: PCT/FI93/00063

(22) International Filing Date: 23 February 1993 (23.02.93)

(30) Priority data:
920792   24 February 1992 (24.02.92)   FI

(71) Applicant (for all designated States except US): NOKIA TE-LECOMMUNICATIONS OY [FI/FI]; Mäkkylän puistotie 1, SF-02600 Espoo (FI).

(72) Inventor; and
(75) Inventor/Applicant (for US only) : MÄENPÄÄ, Sanna [FI/FI]; Otsolahdentie 1 B 22, SF-02110 Espoo (FI).

(74) Agent: OY KOLSTER AB; Stora Robertsgaten 3, P.O. Box 148, SF-00121 Helsinki (FI).

(81) Designated States: AU, GB, JP, NO, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: TELECOMMUNICATION SYSTEM AND SUBSCRIBER AUTHENTICATION METHOD
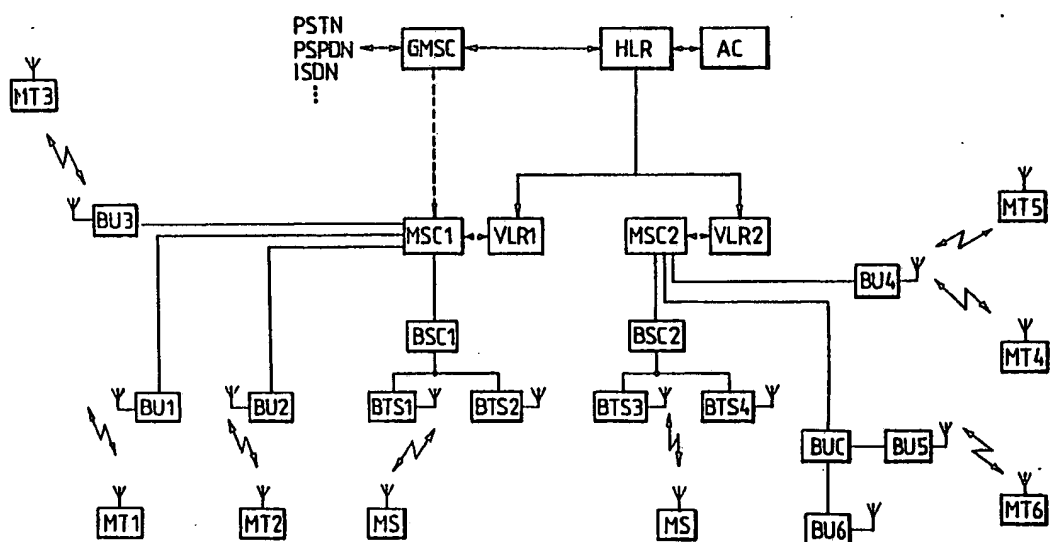
(57) Abstract

The invention relates to a telecommunication system and a method for authenticating a subscriber in a telecommunication system. The system comprises a transmission network having subscriber identity codes of a first format and a first subscriber authentication procedure. An exchange (MSC1, MSC2) of the transmission network is connected to a subsystem having subscriber identity codes of a second format and a second subscriber authentication procedure. The calls of the subscribers (MT1 to MT6) of the subsystem are routed through the transmission network and said exchange (MSC1, MSC2). In the invention, the authentication of both subscriber types is enabled in the transmission network by locating the parameter generation algorithms of both the first and the second authentication procedure in a transmission network authentication centre (AC). The proper algorithm for each subscriber to be authenticated is selected on the basis of the type of the subscriber (MS, MT1 to MT6).

1

Telecommunication system and subscriber authentica-
tion method

Field of the Invention

5   The invention relates a subscriber authentica-
tion method in a telecommunication system comprising
a transmission network having subscriber identity
codes of a first format, a first subscriber authen-
tication procedure and at least one exchange; a sub-
10   system connected to said exchange and having
subscriber identity codes of a second format and a
second subscriber authentication procedure, the calls
of the subscribers of the subsystem being routed
through the transmission network and said exchange,
15   the method comprising the steps: the transmission
network sends an authentication message containing a
first authentication parameter to the subscriber
through the exchange; the subscriber generates a
second authentication parameter in response to the
20   received first authentication parameter and sends it
through the exchange as an authentication response to
the transmission network, and the transmission net-
work compares the second authentication parameter
generated by the subscriber with a corresponding
25   reference parameter and regards the subscriber as
correctly authenticated if the second authentication
parameter and the reference parameter are equal.

Background of the Invention
30   Cordless telephone (CT) systems, such as the
digital cordless telephone system CT2, have recently
been introduced into the market. Such systems com-
prise a base station intended to be connected to a
public switched telephone network (PSTN). There are
35   three different types of base stations: a residential

2

(home) base station, a base station connected to a private branch exchange (PBX) in an office or configured to operate as a PBX, and telepoint base stations, by means of which outward calls only are
5 possible for a CT telephone.

As the present-day CT systems are regarded as PSTN subscriber connections (access points in PSTN), a call is addressed to the CT terminal equipment in a normal way by dialing a telephone number in accord-
10 ance with the PSTN numbering scheme. On the basis of the telephone number the PSTN thereby routes the call to a respective subscriber connection to which the CT residential base station or the PBX of the CT office base station is connected. The base station pages the
15 CT terminal equipment over the radio path by means of an identity code determined by the numbering scheme of the CT system, and sets up a call when the terminal equipment responds. In practice, it is thus possible to make a call to the CT terminal equipment
20 only through its residential or office base stations (through predetermined subscriber connections).

Accordingly, the numbering schemes of the present CT systems themselves serve only the CT radio link and are not utilized anywhere in the PSTN.

25 In the future it may become advantageous to be able to connect CT systems even to mobile radio networks. As there are no addressable access points (such as PSTN subscriber connections) but only common traffic channels shared by all mobile subscriber
30 equipments in the mobile radio network, the setup of a call is always based on the use of an identity code assigned to the subscriber equipment.

A problem therewith is, however, that the numbering schemes specified for the cordless tele-
35 phone system and for the mobile radio system are

3

usually quite different and incompatible. Integrating such systems would require matching of the numbering schemes.

5   In FI Patent Application 914655, to solve this problem, a unique subscriber identity code for the fixed transmission network can be derived from the binary subscriber identity code of the CT system by a simple algorithm at the system interfaces or the same CT subscriber identity code can be restored by an

10   inverse algorithm.

In the mobile radio network, the subscriber identification or authentication is performed at least in connection with the registration to the base station and the call setup. Correspondingly, the

15   authentication procedure is usually performed in the CT systems at least in connection with the call set-up. A problem with the integration of the CT system and the mobile radio system is that their authentication procedures differ from each other and cannot be

20   altered or interconnected so as to be compatible.

Background of the Invention

One object of the invention is to eliminate the above-mentioned problem.

25   This is achieved by means of a method of the type disclosed in the introductory chapter, which according to the invention is characterized in that the transmission network employs for identification of a subscriber of the subsystem a subscriber

30   identity code converted from the second format to the first format and containing a system code indicating that the identity code belongs to a subscriber of the subsystem; the transmission network employs for authentication of a subscriber a pair of the first

35   authentication parameter and the reference parameter,

4

generated according to the authentication procedure
of the transmission system, when a subscriber
identity code belongs to a subscriber of the trans-
mission system; the transmission network employs for
5   authentication of a subscriber a pair of the first
authentication parameter and the reference parameter,
generated according to the authentication procedure
of the subsystem, when a subscriber identity code
belongs to a subscriber of the subsystem.

10   The invention also relates to a telecommunica-
tion system comprising a transmission network having
subscriber identity codes of a first format and a
first subscriber authentication procedure and at
least one exchange; a subsystem connected to said ex-
15   change and having subscriber identity codes of a
second format and a second subscriber authentication
procedure, the calls of the subscribers of the sub-
system being routed through the transmission network
and said exchange. According to the invention the
20   system is characterized in that the parameter gener-
ation algorithms of both the first and the second
authentication procedure are located in an authen-
tication means of the transmission network, the
proper algorithm for each subscriber to be authen-
25   ticated being selectable on the basis of the type of
the subscriber.

          In the invention the subsystem subscriber is
authenticated by the transmission system virtually in
the same way as the subscriber of the transmission
30   network itself except that the transmission network
generates subscriber authentication parameters by
different authentication algorithms, depending on
whether the subscriber is a subsystem subscriber or a
transmission network subscriber. The authentication
35   algorithms of both subscriber types are preferably

5

stored in the authentication units of the transmission network, e.g. in an authentication centre, which reduces processing in the subsystem. The subsystem only transfers authentication requests and responses between the subscriber and the transmission system. In the internal messages and internal functions of the transmission system, the identity of the subsystem subscriber is a subscriber identity code converted so as to comply with the numbering scheme of the transmission network. The identification of the subscriber type and the selection of the appropriate algorithm take place on the basis of a subsystem code contained in the converted subscriber identity. The subsystem authentication data is preferably transferred in the transmission network by utilizing the standard messages and information elements of the transmission system; the subsystem data is incorporated in the existing information elements without changing the format of the element or the structure of the message. In this way, no modifications are required in the transmission system protocols.

Brief Description of the Drawings

In the following the invention will be described in more detail by means of illustrating embodiments with reference to the attached drawings, in which

Figure 1 is a block diagram illustrating a cellular mobile radio system in which the method according to the invention can be applied;

Figure 2 is a flow and block diagram illustrating the numbering scheme conversion method according to the invention in the system of Figure 1;

Figure 3 is a flow and signalling diagram illustrating the authentication procedure according

6

to the CT2 system;

Figure 4 is a flow and signalling diagram illustrating the authentication procedure according to the GSM system; and

5   Figure 5 is a signalling diagram illustrating an authentication procedure of a CT2 system integrated in a GSM system.

Detailed Description of the Invention

10   In the following the invention will be described by means of an example in which a digital cordless telephone system CT2 is integrated in a digital radio telephone system GSM, which is the primary application of the invention. The method

15   according to the invention can, however, also be applied on connecting other cordless telephone systems, such as DECT (Digital European Cordless Telecommunications), to the GSM or its modifications or to other similar mobile radio systems or switched

20   transmission networks.

The basic structure and basic functions of the GSM mobile radio system are well-known to one skilled in the art and relatively accurately defined in the specifications of the GSM system. A reference is also

25   made to The GSM System for Mobile Communications, M. Moyly and M.B. Paulet, Palaiseau, France, 1992; ISBN 2-9507190-0-7. In the following a few basic concepts and elements of the GSM system will be defined with reference to Figure 1. An area within which the GSM

30   mobile radio services are available is called a GSM network (GSM service area), which may cover several countries. The GSM network may be divided into national GSM networks (PLMN service area), i.e. areas covered by one operator offering GSM services. There

35   may also be several GSM networks in the same country

7

and the areas covered by them may overlap geo-
graphically. In the text below, the GSM network
primarily refers to such a "national" network.

The GSM network may comprise one or more MSC
5   areas, i.e. areas within which services are provided
by a single mobile services switching centre MSC
(mobile exchange). The MSC area, in turn, may contain
one or more location areas each covered by one or
more radio cells. The cell is the smallest geo-
10   graphical area of the system, comprising one or more
fixed radio stations, i.e. base stations, and using
predetermined radio channels for communication.

The GSM network comprises at least one home
location register (HLR), which is a data base in
15   which subscriber data, such as location data, are
stored permanently. The HLR also has an associated
authentication centre, which may be integrated or
separate. The authentication centre contains sub-
scriber authentication data and authentication
20   algorithms. The system also comprises several visitor
location registers (VLR) each associated with one or
more MSC areas. However, each MSC area has a single
VLR. The VLR is a data base in which subscriber data
are stored while the mobile station MS visits the
25   area of the VLR. The VLR stores information of the
location of the mobile station MS, normally with the
accuracy of one location area. The HLR, in turn,
stores information of the VLR that the mobile radio
visits and it provides routing data for routing
30   mobile stations MS terminating calls in the network.
The HLR, in turn, receives the required routing data
from the VLR. The HLR and the VLR have only a
signalling connection to the other components of the
mobile radio network.
35   Within the GSM network the subscriber iden-

8

tification is based on the International Mobile Sub-
scriber Identity IMSI, which comprises a GSM Mobile
Country Code MCC (three digits), a Mobile Network
Code MNC (2 digits) of the national GSM network, and
5   a Mobile Station Identification Number MSIN (ten
digits). The MSIN is unique within a certain national
GSM network and can be specified by the network oper-
ator.

     In the example of Figure 1, each MSC area has a
10   dedicated visitor location register VLR associated
with the mobile exchange MSC of the of the respective
MSC area.

     Figure 1 illustrates two MSC areas, one with a
MSC1 and a VLR1 and the other with a MSC2 and a VLR2
15   for the traffic control. There are one or more
location areas under the MSC area covered by the MSC1
and MSC2, respectively, and each location area com-
prises a base station controller BSC1 and BSC2,
respectively, which controls several fixed radio
20   stations, i.e. base transceiver stations BTS. Each
radio cell comprises one BTS, and one base station
controller BTC provides services for several cells. A
mobile station MS located in the cell establishes a
two-way radio link to the BTS of the cell. Both a
25   signalling connection and speech channels are pro-
vided between the BSC and the MSC.

     The GSM network is usually connected to other
networks, such as the public telephone network
(PSTN), another mobile network (PSPDN) or an ISDN
30   network through a MSC called a gateway MSC.

     According to the invention the cordless
telephone system CT2 is integrated as a subsystem for
the GSM system e.g. by connecting CT2 base stations
BU under the control of the MSC. In Figure 1, the CT2
35   base stations BU1, BU2 and BU3 are connected to the

9

MSC1, and the CT2 base stations BU4 and BU5 are con-
nected to the MSC2. The CT2 base station controller
BUC is also connected to the MSC2. In practice, the
BUC may be e.g. a telephone exchange PABX operating
5   in compliance with the CT2 specification and
controlling base stations BU5 - BU6. The mobile
services switching centres MSC and the CT2 base
stations BU and base station controllers BUC are pro-
vided with suitable additional equipment and software
10   for combining the mobility functions of the systems
and for matching the numbering schemes of the
systems.

In principle, the GSM transmission network may
handle CT2 subscribers similarly as actual GSM
15   subscribers although the CT2 and GSM systems are
fully separate radio systems at least on the radio
path level.

The CT2 system and the GSM system, however,
have completely different numbering schemes, and so
20   the CT2 subscriber identity codes cannot be used as
such in the GSM network.

In the CT2 system the CT2 terminal equipment
identity code is a binary 27-bit PID (Portable
Identity Code) which, in turn, comprises two por-
25   tions: an 8-bit MIC (Manufacturer Identity Code) and
a 19-bit HIC (Handset Identity Code). This code is
used in compliance with the CT2 Common Air Interface
(CAI) specification over the radio path between the
CT2 base station BU and the CT2 terminal equipment
30   MT. The CAI specification is described e.g. in *CT2
Common Air Interface*, M.W. Evans, British Tele-
communications Engineering, Vol. 9, July 1990, p.
103-111.

According to the invention, each CT2 terminal
35   equipment is assigned another subscriber identity

10

code for the GSM system, which identity code cor-
responds to the GSM IMSI. This identity code has to
be unique in the GSM network, and it has to be con-
vertible into a CT identity code and again restored
5   at all interfaces between these systems.

Such an identity conversion is described in FI
Patent Application 914655, which is hereby in-
corporated by reference. In   the   following   the
conversion of the PID into the IMSI (PID/IMSI
10   conversion) according to the invention will be de-
scribed briefly with reference to Figure 2: i) A 27-
bit binary PID is converted into a decimal number
(maximum value 134217727), which requires no more
than 9 decimals. ii) A CT2 system identity number N,
15   by means of which the GSM system is able to distin-
guish a CT2 subscriber from GSM subscribers, is added
at a desired position to the 9-decimal number, e.g.
as the most significant number. This results in a 10-
number decimal number which forms an MSIN complying
20   with the GSM specifications. iii) The network code
MNC and the country code MCC are added in front of
the MSIN, thus obtaining an IMSI complying with the
GSM specifications, which can be used as such as a
CT2 terminal equipment identity code in the GSM net-
25   work. The IMSI is converted into the PID (IMSI/PID
conversion) by performing the inverse conversions of
the conversions i - iii in reverse order.

The final IMSI is always formed at the latest
in the MSC, so that the IMSI is used for the CT2
30   terminal equipment everywhere in the GSM network out-
side the MSCs. On the other hand, the PID is always
used over the radio path between the BU and the MT.
The functions required for the PID/IMSI and IMSI/PID
conversions can, in principle, be distributed in any
35   way between the BU or BUC and the MSC.

The subscriber identity code may herein refer to either a subscriber specific identity code or to a terminal equipment specific identity code, depending on the systems to be integrated in each particular case.

Another problem with the interconnecting of the CT2 and GSM systems is that the systems employ different authentication parameters for subscriber identification.

In the CT2 system the authentication is based on the use of a PIN parameter which is stored internally in the CT2 telephone. In the authentication the base station BU compares the PIN parameter from the CT2 telephone MT with the actual PIN parameter of the telephone MT. For safety reasons, the PIN parameter is encrypted for the transmission over the radio path. The CT2 authentication will be described below with reference to Figure 3.

A random number generator 31 of the base station BU generates a 32-bit random challenge RAND (point 32) and sends it in a message AUTH-REQ to a CT2 telephone MT where it is received in the form RAND' (point 32A). The CT2 telephone MT derives a 32-bit CPIN parameter (point 35) from a 64-bit PIN parameter and the parameter RAND' by an encryption algorithm F (point 34). The CPIN parameter is then sent in a message AUTH-RES to the base station BU, which receives it in the form CPIN' (point 35A). The base station BU deduces the value of a parameter E-PIN (expected-PIN) associated with the telephone MT by means of identification information (point 37) and calculates the value of a parameter E-CPIN (expected CPIN) (point 31) from the parameters E-PIN and RAND by means of the algorithm F (point 38). The BU compares the obtained value CPIN' with the value E-CPIN

12

and if the values are equal, the authentication has been accomplished properly.

In the GSM system, the MSC may request authentication parameters for each subscriber MS from the authentication centre AC of the subscriber's MS home network by sending a message SEND-PARAMETERS. The authentication centre is either a separate unit or integrated in the HLR, as illustrated in Figure 1. The authentication centre AC selects a subscriber specific authentication key K_i on the basis of the subscriber identity code IMSI contained in the message SEND_PARAMETERS. In addition, a random number generator 42 generates a plurality of random number parameters RAND (point 43), from which and the key K_i a reference parameter SRES is derived by an authentication algorithm A3 (point 44) for each parameter RAND (point 45). The authentication centre AC sends these RAND/SRES pairs in a message SEND_PARAMETERS to the VLR, in which they are stored in a subscriber specific RAND/SRES table (point 46).

When the VLR authenticates the subscriber identity code, it selects a value for the parameter RAND from the RAND/SRES table of this subscriber and sends the value in a message AUTHENTICATE to the MSC, which forwards it in a message AUT_REQUEST to the subscriber MS (point 47). The subscriber MS comprises the same authentication key K_i and authentication algorithm A3 as those used in the authentication centre AC. The subscriber MS calculates the parameter SRES (50), which is the authentication response of the MS, by utilizing the parameter RAND received by it (point 47), the key K_i (point 48) and the algorithm A3 (point 49). The MS returns the parameter SRES to the MSC in a message AUT_RESPONSE, and the MSC forwards it in a message AUTHENTICATION_RESPONSE to the

13

VLR. The VLR compares (point 52) the value SRES sent by the MS with the stored value SRES (point 51), and if they are equal, the authentication has been accomplished properly.

5   The above-described authentication procedures of the CT2 and GSM systems cannot be altered or integrated so as to achieve compatibility. This is due to the randomness of the identification responses E-PIN, CPIN and SRES to be calculated by the authen-
10   tication algc 'thms F and A3, wherefore the algorithms do ι. : yield linear results. In order to accomplish propθ¬ authentication between a CT2 sub-scriber and the ˙3M transmission network, the trans-missi.ι network also has to be able to perform the
15   authentication procedure in compliance with the CT2 system.

        In the invention, this is achieved by incorpor-ating the CT2 authentication algorithm F, the random number generator 31 and the algorithm 37 for deriving
20   the parameter E-pin, located in the base station BU in Figure 3, in the authentication centre AC of the GSM system. The AC is capable of selecting the appropriate authentication algorithm on the basis of the subscriber identity code of the subscriber to be
25   identified. CT2 subscribers, for instance, can be distinguished from ordinary GSM subscribers by means of a CT2 specific decimal number N contained in the MSIN field of the IMSI code assigned to the CT2 sub-scriber, as described above with reference to Figure
30   2. In addition to the CT2 authentication algorithm, it is possible that the authentication centre AC also comprises a table containing the authentication algorithms and random number generators of other sub-systems that may be connected to the GSM transmission
35   network. Accordingly, an appropriate one of the

14

authentication algorithms can be selected for each subscriber type on the basis of the subscriber identity code, and the authentication parameters generated by each authentication algorithm are trans-
5   ferred to the VLR. The selection of the authentica-
tion algorithm does not affect the signalling protocol or the structure of messages in the GSM system but CT2 specific authentication data is trans-ferred in the GSM network by standard GSM messages
10   and information elements without changing the format of the information elements or the message format. As CT2 data is typically shorter than GSM data, the un-occupied space of the GSM information elements is filled with zeros in conjunction with CT2 data.

15   The authentication of a CT2 subscriber in the GSM system in accordance with the invention will be described below by way of example. Table I lists the messages, functions, protocol types and information elements used in Figure 5. The table also refers to
20   the page number of the respective GSM or CT2 specifi-cation so that B refers to the GSM specification 09.02, and E or A refers to the CT2 specification ETSI TC/RES I-ETS[???].

Referring to Figure 5 and Table I, the authen-
25   tication according to the invention will be described by dividing it into the functions 631, 641, 651, 542, 532, 621, 611, 622, 633 and 643.

631) The MSC initiates the authentication by sending the VLR one of the MAP messages used for
30   starting authentication. This message may be e.g. PRO_ACC_REQ. An appropriate authentication algorithm is selected on the basis of the subscriber type. The subscriber type is determined by analyzing the IMSI code.

35   641) After having received the authentication

15

initiation message, the VLR may, if required, request
the authentication centre AC of the HLR to send
authentication parameters. However, this is not
always necessary. If the VLR has a sufficient number

5   of stored authentication parameters left from the
previous request (cf. Figure 4), it does not need to
request more parameters. Such a request is made by
sending the message SEND_PARAMETERS to the HLR/AC.
This message consists of the Request Parameter

10   information elements and complies with the MAP
protocol. It contains the following parameters:
REQUEST, IMSI, AuthenticationSet, SubscriberData, CUG
information and K_i. When the message is sent, the
timer having a timing period of 15 to 30 seconds is

15   started. The timer is stopped when the message
SEND_PARAMETER is received.

        651) On receiving the message SEND_PARAMETERS
the authentication centre of the HLR analyses the
IMSI code of the subscriber to find out whether CT2

20   specific or GSM specific data is required. For a CT2
subscriber, a CT2 specific authentication algorithm
is used to perform a calculation operation after
which the HLR/AC returns the requested parameter
results in the message SEND_PARAMETERS. This message

25   complies with the MAP protocol. The requested para-
meters may be IMSI, AuthenticationSet, Subscriber-
Data, CUG information and the key K_i.

        AuthenticationSet = SEQUENCE[RAND, CPIN, K_c].

        RAND is a random number used in the authentica-

30   tion. It is CT2 specific and shorter than the GSM
specific random number RAND.

        CPIN is a 32-bit result of the CT2 algorithm
performed by the AC of the subscriber, corresponding
to the parameter E-CPIN of Figure 3.

35   K_c is an encryption key; it is not used in this

16

specific case.

642) After having received the message
SEND_PARAMETERS the VLR initiates the authentication
procedure by sending the message AUTHENTICATE to the
5   MSC. The message complies with the MAP protocol. It
contains the information elements RAND and cksn. Cksn
stands for an encryption key sequence number which is
not used in the CT2 authentication procedure as it is
not relevant to the CT2 system. On transmitting this
10   message, the VLR starts a T-aut counter the time
value of which is 5 to 10 seconds. The timer is
stopped when the VLR receives the message
AUTHENTICATION_RES.

632) The MSC maps the message AUTHENTICATE so
15   that it complies with the MM' protocol and transfers
a message CM_AUT_REQ to the CT2 base station BU. This
message has to contain the parameter RAND as well.

621) The base station BU maps the message
CM_AUT_REQ in the message AUTH_REQ, which complies
20   with the protocol format of the layer 3 of the CT2
system. This authentication request information
element comprises two parameters, RAND and INCZ. The
message AUTH_REQ is sent to the telephone MT.

611) The telephone MT receives the message
25   AUTH_REQ and performs the required authentication
algorithms. Then it responds with the message
AUTH_RES, which complies with the CT2 protocol. This
authentication response information element contains
three parameters, CPIN, ZAP and TRD.

30   ZAP represents the content of a 4-bit ZAP field
stored in the mobile telephone MT. The operator may
use it as part of the overall authentication process
of the telephone MT. When the INCZ of the received
message AUTH_REQ is set to one, it causes the MT to
35   increment the content of the 4-bit ZAP field (modulo-

17

16). When the INCZ is set to zero, the field remains unchanged.

The TRD field is used to transfer charging data associated with the CT2 system. The use and inter-
5   pretation of data in this field can be selected by the operator. The TRD is an optional field of variable length, which may contain 23 BCD numbers.

622) On receiving the message AUTH_RES the base station BU maps the message in the message
10   CM_AUT_RES, which is sent to the MSC. The last-mentioned message complies with the MM' protocol and it has to contain the CT2 specific CPIN parameter.

633) The MSC receives the message CM_AUT_RES and maps it in the message AUTHENTICATION_RES comply-
15   ing with the MAP protocol. The AUTHENTICATION_RES contains said calculated authentication parameter CPIN and is sent to the VLR.

643) The VLR compares the received authentica-tion parameter CPIN with its internal parameter CPIN,
20   which is calculated and sent to the VLR by the AC. If the parameters are equal, the authenticity of the MT has been proved.

In place of storing and performing the algo-rithms merely in the authentication centre AC, at
25   least part of the authentication algorithms may be located in and performed by the VLR, whereby the authentication centre AC sends the VLR only the encryption key K_i in the message SEND_PARAMETERS. This is another way of processing the identification key
30   specified in the GSM network, which, however, is not as safe as that described by way of example, as the key K_i transferred to and known at several different locations in the network.

The authentication algorithms and functions may
35   also be distributed in another way in the GSM net-

18

work, though it may thereby be necessary to deviate
from the specifications of the GSM network.

    The attached figures and the description
related to them are only intended to illustrate the
5   present invention. In its details, the method and
system according to the invention may vary within the
spirit and scope of the attached claims.

TABLE I

Name of Message	Func-tion Number	Type of Proto-col	Information Elements	Refer-ences
[Message]	641	MAP	-	-
SEND-PARA-METERS	651	MAP	REQUEST:IMSI, Authentication-Set, Subscriber-Data, CUG-In-formation, Ki	Bp300, 463
SEND-PARA-METERS	642	MAP	IMSI, Authentica-tionSet, SubscriberData, CUG-Information, Ki	Bp300, 463
Authen-ticate	632	MAP	RAND, cksn	Bp292, 422
CM-AUT-REQ	621	MM'	RAND	-
AUTH-REQ	611	CT2/ layer3	RAND, INCZ, Auth-no	Ap3-18, Ep70
AUTH-RES	622	CT2/ layer3	CPIN, ZAP, TRD, OPSIC, TCOS	Ap3-19, Ep71
CM-AUT-RES	633	MM'	CPIN	-
AUTHEN-TICATION-RES	643	MAP	CPIN	Bp292, 422

20

Claims:

1. Subscriber authentication method in a tele-
communication system comprising a transmission net-
work having subscriber identity codes of a first
format, a first subscriber authentication procedure
and at least one exchange; a subsystem connected to
said exchange and having subscriber identity codes of
a second format and a second subscriber authentica-
tion procedure, the calls of the subscribers of the
subsystem being routed through the transmission net-
work and said exchange, the method comprising the
steps:
        the transmission network sends an authentica-
tion message containing a first authentication para-
meter to the subscriber through the exchange;
        the subscriber generates a second authentica-
tion parameter in response to the received first aut-
hentication parameter and sends it through the
exchange as an authentication response to the trans-
mission network, and
        the transmission network compares the second
authentication parameter generated by the subscriber
with a corresponding reference parameter and regards
the subscriber as correctly authenticated if the
second authentication parameter and the reference
parameter are equal, c h a r a c t e r i z e d   in
that
        the transmission network employs for iden-
tification of a subscriber of the subsystem a sub-
scriber identity code converted from the second
format to the first format and containing a system
code indicating that the identity code belongs to a
subscriber of the subsystem;
        the transmission network employs for authen-

tication of a subscriber a pair of the first authentication parameter and the reference parameter, generated according to the authentication procedure of the transmission system, when a subscriber identity code belongs to a subscriber of the transmission system;

the transmission network employs for authentication of a subscriber a pair of the first authentication parameter and the reference parameter, generated according to the authentication procedure of the subsystem, when a subscriber identity code belongs to a subscriber of the subsystem.

2. Method according to claim 1, c h a r a c - t e r i z e d in that said converted subsystem subscriber identity code and said authentication parameters are transferred in the transmission network in the normal authentication messages of the transmission network.

3. Authentication method according to claim 1 or 2, c h a r a c t e r i z e d in that

the switching centre initiates the authentication by transmitting an authentication request containing the subscriber identity code of the subscriber to the authentication means of the transmission network;

the authentication means verify by means of said system code whether the subscriber identity code is a subsystem subscriber identity code or transmission network subscriber identity code;

the authentication means send an authentication message to the exchange, the authentication message containing the first authentication parameter generated by the authentication algorithm of the transmission network if the subscriber identity code of the authentication request is a transmission network sub-

22

scriber identity code, or generated by the authen-
tication algorithm of the subsystem if the subscriber
identity code of the authentication request is a sub-
system subscriber identity code;

5   the exchange sends the subscriber a second
authentication request containing said first authen-
tication parameter;

the subscriber generates a second authentica-
tion parameter on the basis of the received first
10   authentication parameter, and sends the second
authentication parameter as an authentication
response to the exchange and further to the authen-
tication means;

the authentication means compare the second
authentication parameter generated by the subscriber
with a corresponding reference parameter and if the
parameters are equal, the subscriber is regarded as
5   correctly authenticated.

4. Method according to claim 3, wherein the
transmission network is a cellular mobile network in
which said authentication means comprise at least one
authentication centre and a visitor location register
10   associated with the exchange, c h a r a c t e r i z -
e d   in that on receiving an authentication request
from the exchange the visitor location register sends
the authentication centre a parameter request con-
taining the subscriber identity code;

15   the authentication centre verifies whether the
subscriber identity code is a transmission network
identity code or a subsystem subscriber identity code
and then performs, on the basis thereof, the trans-
mission network or subsystem authentication algo-
20   rithm, respectively, so as to generate at least one
pair of the first parameter and the reference para-
meter for the subscriber;

23

the authentication centre sends said at least one parameter pair to the visitor location register;

the visitor location register sends the subscriber the first authentication parameter through

5   the exchange; and

the visitor location register compares the second authentication parameter generated by a remote station with a corresponding reference parameter and if the parameters are equal, the authentication has

10   been accomplished properly.

5. Method according to claim 4, c h a r a c -
t e r i z e d in that the authentication centre sends the visitor location register a plurality of subscriber specific parameter pairs which are stored

15   in the visitor location register for subsequent authentications of the same subscriber.

6. Telecommunication system comprising

a transmission network having subscriber identity codes of a first format and a first subscriber

20   authentication procedure and at least one exchange (MSC1, MSC2);

a subsystem connected to said exchange and having subscriber identity codes of a second format and a second subscriber authentication procedure, the

25   calls of the subscribers of the subsystem being routed through the transmission network and said exchange (MSC1, MSC2), c h a r a c t e r i z e d in that the parameter generation algorithms of both the first and the second authentication procedure are

30   located in an authentication means (AC) of the transmission network, the proper algorithm for each subscriber to be authenticated being selectable on the basis of the type of the subscriber (MS, MT1 to MT6).

35   7. Telecommunication system according to claim

24

6, c h a r a c t e r i z e d   in that the subsystem
is a cordless telephone system.

       8. Telecommunication system according to claim
7, c h a r a c t e r i z e d in that the transmission
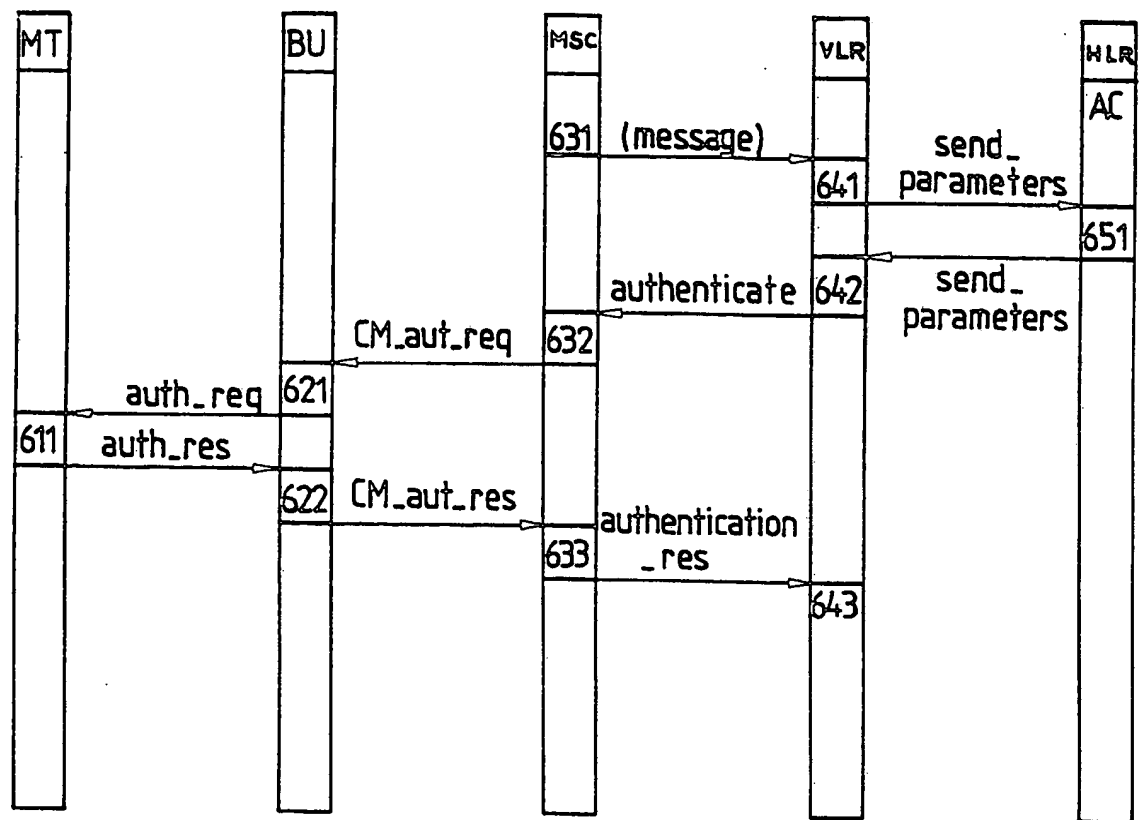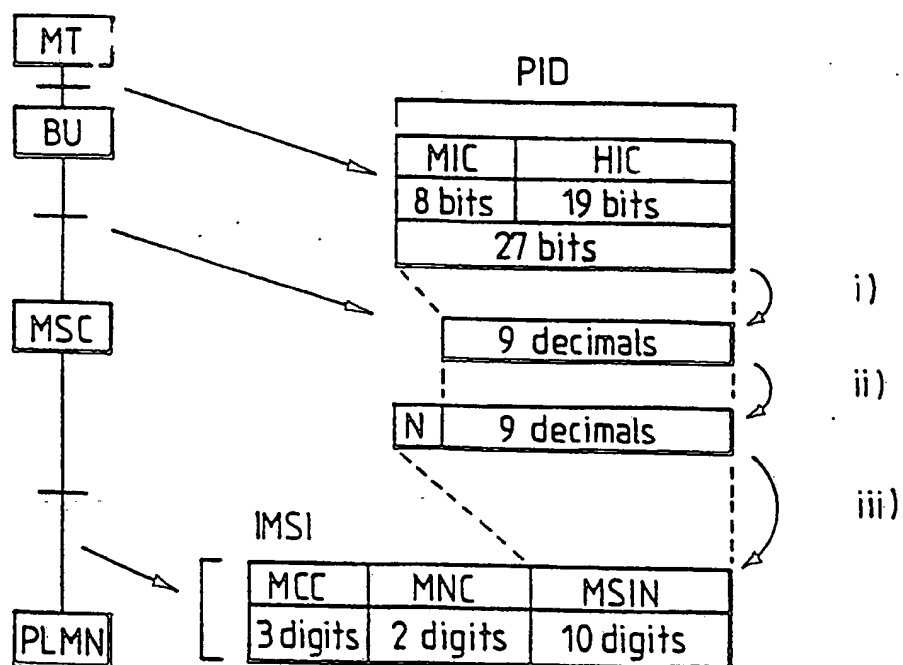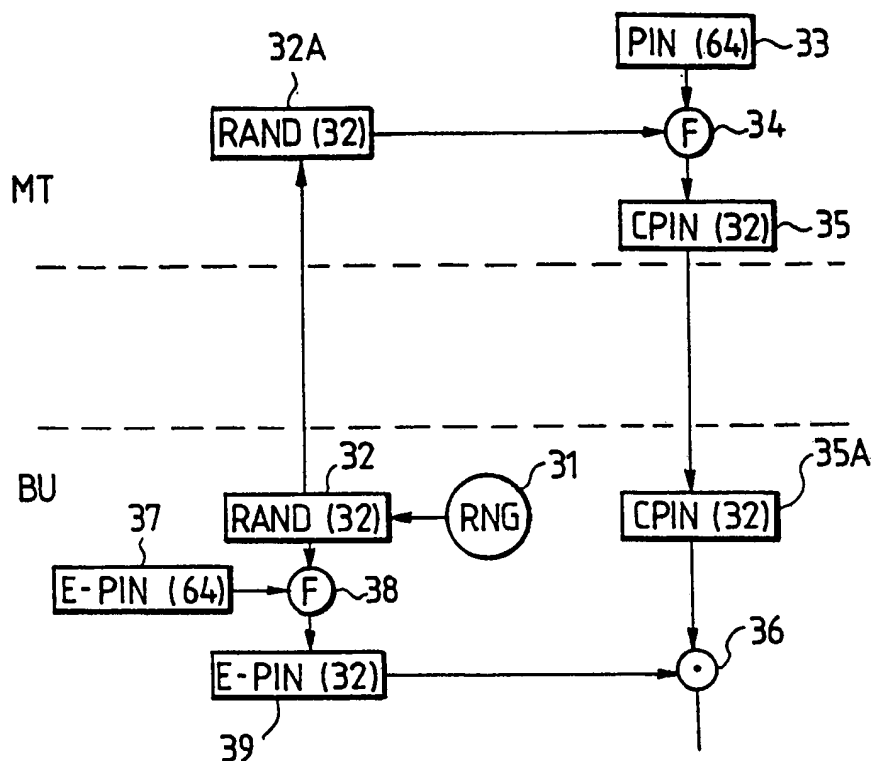network is a mobile radio system.
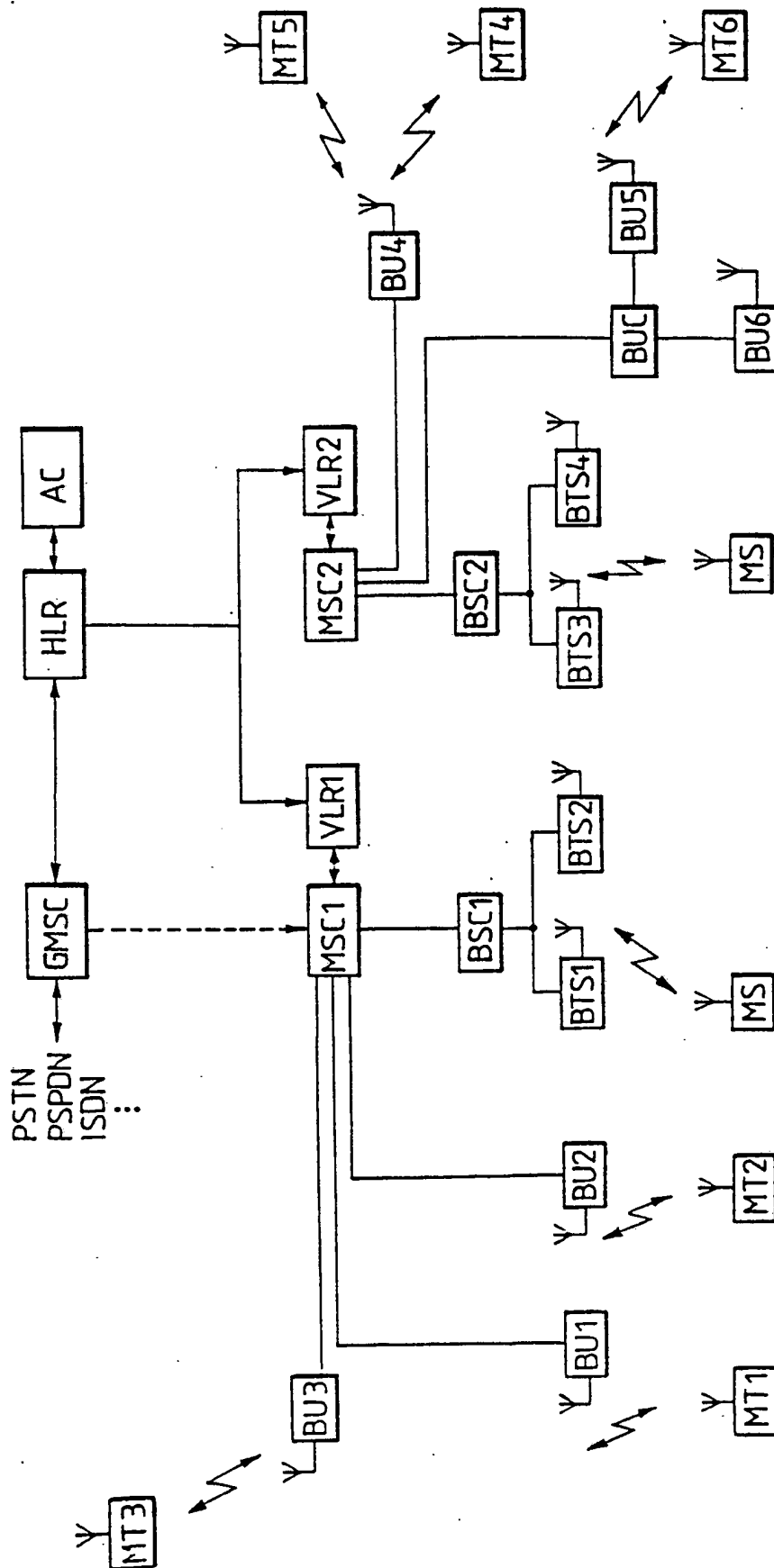
FIG. 1

FIG. 5

FIG. 2

FIG. 3

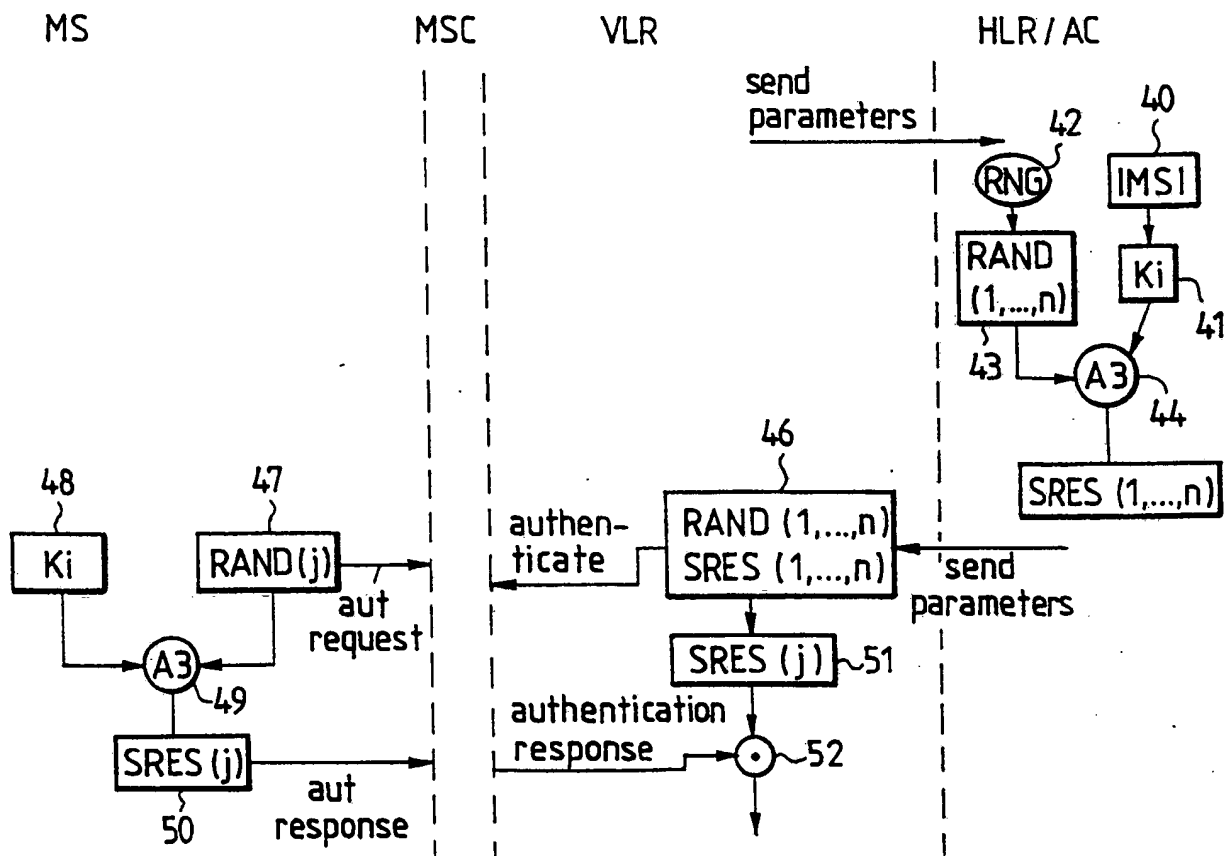
FIG. 4

A. CLASSIFICATION OF SUBJECT MATTER

IPC5: H04Q 7/04, H04B 7/26
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC5: H04Q, H04B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

DIALOG: 2,125,340,350,351

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	WO, A1, 9307721 (NOKIA TELECOMMUNICATIONS OY), 15 April 1993 (15.04.93), page 2, line 19 - line 26, figure 1	1-8
A	WO, A1, 9015488 (MOTOROLA, INC.), 13 December 1990 (13.12.90), page 3, line 29 - page 4, line 18, claim 8	1-8
P,A	GB, A, 2257334 (AMERICAN TELEPHONE AND TELEGRAPH COMPANY), 6 January 1993 (06.01.93), figure 1, abstract	1-8

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	
"E" erlier document but published on or after the international filing date	"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 May 1993	03 -06- 1993
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Margareta Nylander Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 5020093 (ALI PIREH), 28 May 1991 (28.05.91), claim 1, abstract	1-8

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO-A1- 9307721	15/04/93	NONE		
WO-A1- 9015488	13/12/90	AU-B-	634234	18/02/93
		AU-A-	5539290	07/01/91
		CN-A-	1047952	19/12/90
		EP-A-	0474675	18/03/92
		JP-T-	4506138	22/10/92
		US-A-	5095529	10/03/92
		CA-A-	2057911	01/12/90
		US-A-	5159695	27/10/92
GB-A- 2257334	06/01/93	NONE		
US-A- 5020093	28/05/91	CA-A-	2016333	23/12/90
		CA-A-	2019000	23/12/90
		JP-A-	3035626	15/02/91
		JP-A-	3035628	15/02/91
		CA-A-	2022278	28/04/91
		US-A-	5008925	16/04/91